AMENDMENTS IN THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF THE CLAIMS:

1. (Currently amended) A method of responding to the detection of an intrusion on a network system that provides network services, the network system including one or more attached functions and a plurality of interconnection devices, the method comprising the steps of:

a. providing means for one or more attached functions to connect to one or more of a plurality of interconnection devices of the network system;

b. acquiring information about the attached functions seeking access to the network services;

c. determining whether one or more stored policies exist for the attached functions;

d. allowing at least one of the one or more attached functions to access a selectable portion of the network services based on a policy established in one or more of the interconnection devices;

e. monitoring the network system for intrusions;

f. excluding from at least one of the plurality of interconnection devices a policy enforcement module for effecting its own signal transfer policy changes;

g including in at least one of the plurality of interconnection devices the capability for such interconnection device to change directly its own signal transfer policies;

hg. upon detection of one or more intrusions of the network,

i. determining a physical address or a logical address for each attached function associated with the source of the intrusion; and

ii. identifying one or more interconnection devices having a policy enforcement module and used by the identified attached function or functions to gain access to the network services;

ih. selectively changing one or more signal transfer policies of one or more of the plurality of interconnection devices in response to the one or more detected intrusions; and

jj. saving changed policies for the one or more attached functions.

2. CANCELED.

3. (Previously presented) The method as claimed in Claim 1 wherein the physical address information is a MAC address or the logical address information is an IP address.

4. CANCELED.

5. (Previously presented) The method as claimed in Claim 4 further comprising the step of employing an intrusion detection device of the network system to perform the function of detecting the one or more intrusions, wherein the intrusion detection device is either a centralized network system device, a plurality of distributed network system devices or a combination of both.

6. CANCELED.

7. CANCELED.

8. (Previously presented) The method as claimed in Claim 1 wherein the step of identifying the interconnection device used by the attached function includes the step of determining the physical address, logical address, or both for the interconnection device.

9. (Currently amended) The method as claimed in Claim [[2]]1 further comprising the step of verifying the identification of the identified source of the intrusion.

10. (Previously presented) The method as claimed in Claim 1 wherein the step of selectively changing one or more signal transfer policies of one or more of the plurality of interconnection devices in response to the one or more detected intrusions includes the step of configuring the one or more interconnection devices to perform one or more functions selected from the group consisting of: blocking complete access to the network services by an identified source of a

detected intrusion, blocking access by identified logical addresses only, blocking access by an identified access protocol only, limiting bandwidth, limiting exchanges to or from the one or more interconnection devices, to or from one or more other devices of the network system, or to or from any of the attached functions not identified as an intrusion source, and directing all signals exchanged by the identified sources to a honeypot, an intrusion detection device, a monitoring device, or a simulation device.

11. (Previously presented) The method as claimed in Claim 1 wherein the step of selectively changing one or more signal transfer policies of one or more of the plurality of interconnection devices in response to the one or more detected intrusions includes the step of configuring the one or more interconnection devices to permit connectivity of an identified source of a detected intrusion while dampening the level of activity associated with the identified source to minimize network harm while permitting analysis and auditing of the identified source and the gathering of forensic evidence.

12. (Previously presented) The method as claimed in Claim 1 wherein the step of selectively changing one or more signal transfer policies of one or more of the plurality of interconnection devices in response to the one or more detected intrusions includes the steps of first configuring a first set of the one or more interconnection devices with a first set of one or more policy changes, monitoring the network system for intrusions and, upon detection of one or more intrusions related to the intrusions causing the first one or more policy changes, configuring a second set of the one or more interconnection devices with a second set of one or more policy changes.

13. (Previously presented) The method as claimed in Claim 12 wherein one or more of the one or more interconnection devices of the second set are interconnection devices of the first set.

14. (Previously presented) The method as claimed in Claim 1 wherein the one or more interconnection devices are network entry devices.

15. (Previously presented) The method as claimed in Claim 1 wherein the one or more signal transfer policy changes are configured on one or more ports of the identified interconnection devices associated with the source of the intrusion.

Claims 16-28: CANCELED.

29. (Previously presented) The method as claimed in Claim 1 further comprising the step of verifying the identification of the identified source of the intrusion.

30. (Currently amended) A network system including a plurality of attached functions, and the network system including the capability to respond to intrusions thereof, the network system comprising:

a. an intrusion detection function for identifying one or more sources of one or more intrusions of the network system;

b. a plurality of interconnection devices for transferring signals through the network system, wherein each of the plurality of interconnection devices includes one or more signal transfer policies, wherein at least one of the plurality of interconnection devices includes the function to change directly its own signal transfer policies;

c. a function of a policy enforcement module to change selectively the signal transfer policies of one or more of the plurality of interconnection devices in response to the one or more detected intrusions, wherein at least one of the plurality of interconnection devices excludes the policy enforcement module to establish therein the function to change selectively its own signal transfer policies;

d. means to connect one or more attached functions to one or more of the plurality of interconnection devices;

e. a function to determine whether a stored policy history exists for the one or more attached functions;

f. one or more policies established on one or more of the interconnection devices to allow at least one of the one or more attached functions to access a selectable portion of the network services;

g. a function to determine a physical address or a logical address for the attached function or attached functions identified by the intrusion detection function as the source or sources of the one or more intrusions;

h. a function to identify the one or more interconnection devices having the policy enforcement module and used by the one or more identified attached functions to gain access to the network services; and

i. a function to save modified policies for the one or more attached functions.

31. (Withdrawn) The network system as claimed in Claim 30, wherein at least one of the interconnection devices has no intrusion detection function and wherein the signal transfer policies of that at least one of the plurality of interconnection devices cannot be changed in response to the one or more detected intrusions.

32. CANCELED.

33. (Previously presented) The network system as claimed in Claim 30 further comprising a directory service function for receiving address information for the attached functions and the interconnection devices.

34. (Previously presented) The network system as claimed in Claim 33 further comprising a policy manager function for configuring the plurality of interconnection devices with the signal transfer policies.

35. (Previously presented) The network system as claimed in Claim 34 further comprising a policy decision function configured:

a. to receive detected intrusion information from the intrusion detection function;

b. to receive information from the directory service function;

c. to evaluate whether a policy change or changes is or are required on one or more of the interconnection devices in response to the detected intrusion information; and

d. to direct the policy manager function to configure one or more of the plurality of interconnection devices with determined policy changes upon deciding to do so based upon the evaluation.

36. (Previously presented) The network system as claimed in Claim 35 wherein the policy manager function and the policy decision function are part of a centralized server.

37. (Previously presented) The network system as claimed in Claim 36 wherein the directory service function is part of the central server.

38. (Previously presented) The network system as claimed in Claim 30 wherein the intrusion detection function is a centralized intrusion detection function or a distributed intrusion detection function.

39. (Previously presented) The network system as claimed in Claim 30 wherein the one or more of the plurality of interconnection devices selected for signal transfer policies changes are network entry devices selected based on their local connection to the one or more sources of the one or more intrusions.

40. (Previously presented) The network system as claimed in Claim 30 further comprising a network management system for identifying address information for the plurality of interconnection devices.

41. (Previously presented) The network system as claimed in Claim 30 further comprising a function to validate the accuracy of the identity of the identified one or more sources including a logical address, a physical address, or a location.

42. (Previously presented) The method as claimed in Claim 1wherein the identified attached function gains access to the network services through one of the interconnection devices to which it is directly connected.

43. (Previously presented) The method as claimed in Claim 1 further comprising the step of establishing one or more policies for the one or more attached functions without communicating with a centralized policy server.

44. (Previously presented) The network system as claimed in Claim 30 wherein the one or more identified attached functions gain access to the network services through one of the interconnection devices to which they are directly connected.

45. (Previously presented) The network system as claimed in Claim 30 wherein the policy enforcement module is configured to establish one or more policies for one or more of the one or more attached functions without communicating with a centralized policy server.

46. (Currently amended) The method as claimed in Claim [[4]] 1 wherein the at least one of the plurality of interconnection devices further includes an intrusion detection function.